WHAT IS CLAIMED IS:

1. A method for countering unauthorized decryption comprises a step of scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing.

2. The method for countering unauthorized decryption according to Claim 1, wherein the hardware operational phenomenon is power consummated by the hardware to execute the data decryption processing.

3. The method for countering unauthorized decryption according to Claim 1, wherein the hardware is a IC card, a PDA, or a cellular phone.

4. The method for countering unauthorized decryption according to Claim 1, wherein the data decryption processing is executed to decrypt data encrypted by a RSA encryption processing or an elliptic encryption processing.

5. The method for countering unauthorized decryption according to Claim 1, wherein the correlation is scrambled by an arithmetic operation method implemented by an information processing apparatus comprising the steps of:

for two integers K1 and K2, when finding a value F(K, A) of a function F satisfying F(K1+K2, A)=F(K1, A) ○F(K2, A) (○ denotes an arithmetic operation in a communtative semigroup S. K designates an integer and A designates an

element of S), decomposing the K to the sum of m integers K[0] + K[1] + ... K[m-1];

using T(0), T(1), ... T(m-1) resulted from rearranging a string of integers 0, 1, ... m-1 by permutation T; and

operating on terms F(K[T(0)], A) to F(K[T(m-1)], A) on the right side of F(K, A) = F(K[T(0)], A) ○F(K[T(1)], A) ○ ...F(K[T(m-1)], A) ... ("expression 1") in an order of F(K[T(0)], A), F(K[T(1)], A), ... F(K[T(m-1)], A) to find F(K, A).

6. The method according to claim 5, whereby the permutation processing, the permutation T prevents predicting any post-permutation data from pre-permutation data, or the permutation T is performed based on a dummy random number, and whereby the permutation processing is performed each time the expression 1 is performed.

7. The method according to claim 5, wherein the S is a commutative semigroup in which, for a set consisting of residues by an integer N (N ≥ 2), the arithmetic operation ○ of a modular multiplication operation A○B=A*B mod N is introduced, and the F satisfies F(K, A)=A^K mod N (A^K denotes the K-th power of A).

8. The method according to claim 5, wherein the information processing apparatus is installed on an IC card, a cellular phone, or a PDA.

9. The method according to claim 7, wherein the integer K is split in a form of

$K[j] = u*((2^t)^j)$ $(0 \leq u \leq (2^t)-1,\ t = 1,2,....)$

10. The method according to claim 9, whereby the permutation processing, the permutation T is performed based on an information source prevents predicting any post-permutation data from pre-permutation data, or the permutation T is performed based on a dummy random number, and whereby the permutation processing is performed each time the expression 1 is performed.

11. The method according to claim 9, wherein the integer K is split in a form of $K[j] = u*((2^t)^j)$ $(0 \leq u \leq (2^t)-1,\ t = 1,2,....)$

12. The method according to claim 5, wherein the S is a Mordell-Weil group on an elliptic curve E defined on a finite field GF(p) (p is a prime number) or GF(2^n) (n is an integer equal to or greater than 1), and an expression F(K,A)=KA is satisfied, wherein the A denotes a point on the elliptic curve E, the KA denotes the arithmetic operation ○ performed on K number of As such that the KA denotes A ○A○A ... ○A (K number) when the K is positive, or (-A)○(-A)○(-A) ... ○ (-A) (|K| number) when the K is negative, and 0 (the point at infinity) on the E when the K is 0, the ○ denotes an addition operation in the Mordell-Weil group, and the -A is an inverse in the Mordell-Weil group of the A.

13. The method according to claim 12, wherein the information processing apparatus is installed on an IC card.

14. The method according to claim 12, wherein the integer K is split in a form of

$K[j] = u*((2^t)^j)$ $(0 \leq u \leq (2^t)-1, t = 1,2,....)$

15. The method according to claim 14, wherein the information processing apparatus is installed on an IC card.

16. An apparatus for countering unauthorized decryption comprises means for scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing.

17. The apparatus for countering unauthorized decryption according to Claim 16, wherein the hardware operational phenomenon is power consummated by the hardware to execute the data decryption processing.

18. The apparatus for countering unauthorized decryption according to Claim 16, wherein the hardware is a IC card, a PDA, or a cellular phone.

19. A software product for countering unauthorized decryption comprises a module for scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing.

20. The software product for countering unauthorized decryption according to

Claim 19, wherein the hardware operational phenomenon is power consummated by the hardware to execute the data decryption processing.